

# **Exhibit B**

**SCHEDULE "A"**

**Amended pursuant to Rule 6-1(1)(a) of the Supreme Court Civil Rules.  
Original Notice of Civil Claim filed on October 20, 2023**

**NO. S-237147**

**VANCOUVER REGISTRY**

**IN THE SUPREME COURT OF BRITISH COLUMBIA**

**BETWEEN:**

**J. R. and M. M.**

**PLAINTIFFS**

**AND:**

**23ANDME HOLDING CO., 23ANDME, INC.,  
ANNE WOJCICKI, ROELOF BOTHA, PATRICK CHUNG,  
PETER J. TAYLOR, DAVID BAKER and KPMG LLP (UNITED STATES)**

**DEFENDANTS**

**[PROPOSED] AMENDED NOTICE OF CIVIL CLAIM**

**Brought under the *Class Proceedings Act*, RSBC 1996, c. 50**

**This action has been started by the Plaintiffs for the relief set out in Part 2 below.**

If you intend to respond to this action, you or your lawyer must

- (a) file a response to civil claim in Form 2 in the above-named registry of this court within the time for response to civil claim described below, and
- (b) serve a copy of the filed response to civil claim on the plaintiff.

If you intend to make a counterclaim, you or your lawyer must

- (a) file a response to civil claim in Form 2 and a counterclaim in Form 3 in the above-named registry of this court within the time for response to civil claim described below, and
- (b) serve a copy of the filed response to civil claim and counterclaim on the plaintiff and on any new parties named in the counterclaim.

JUDGMENT MAY BE PRONOUNCED AGAINST YOU IF YOU FAIL to file the response to civil claim within the time for response to civil claim described below.

**Time for response to civil claim**

A response to civil claim must be filed and served on the Plaintiff,

- (a) if you were served with the notice of civil claim anywhere in Canada, within 21 days after that service,
- (b) if you were served with the notice of civil claim anywhere in the United States of America, within 35 days after that service,
- (c) if you were served with the notice of civil claim anywhere else, within 49 days after that service, or
- (d) if the time for response to civil claim has been set by order of the court, within that time.

[the balance of this page has been intentionally left blank]

## CLAIM OF THE PLAINTIFFS

### PART 1: STATEMENT OF FACTS

#### A. Overview

1. This proposed privacy class action arises out of a data breach that affected the customers of 23andMe Holding Co. and 23andMe, Inc. (collectively, “**23andMe**” or “**23andMe Defendants**”) in 2023 (hereinafter, “**Data Breach**”).
2. The Data Breach occurred over the span of approximately five months—between April 29 and September 27, 2023. And it resulted in the theft or compromise of highly sensitive and highly valuable personal information of millions of customers of 23andMe, including information regarding their ethnicities, religious backgrounds, ancestry roots and connections, and genetics. Information of millions of 23andMe customers was posted for sale on the Dark Web.
3. This action arises out of two main allegations:
  - a. **IMPROPER DATA RETENTION MEASURES AND PRACTICES:** first, that contrary to their promises, statements and representations, as well as the standards applicable to them by virtue of privacy regulation and practices, the 23andMe Defendants did not introduce, implement and/or maintain proper data retention practices. As a result, they retained a significant volume of highly sensitive customer information outside of the scope of their authorization; and
  - b. **IMPROPER DATA PROTECTION MEASURES AND PRACTICES:** second, that contrary to their promises, statements and representations, as well as the standards applicable to them by virtue of privacy regulation and industry practices, the 23andMe Defendants did not introduce, implement and/or maintain proper data protection measures and/or practices. As a result, they affirmatively exposed the highly sensitive and highly valuable

customer data in their control, custody or possession to unauthorized parties and cybercriminals.

4. The 23andMe Defendants failed to conduct their data retention and protection practices appropriate to the sensitivity of the customer information in their power, custody or possession, or the severity of the risk of cyberattacks. The 23andMe Defendants' actions and omissions in breach of their duties were deliberate and purposeful, and were carried out in the normal course of the 23andMe Defendants' commercial activities and in furtherance of their business interests.
5. The Individual Defendants (as defined below) and KPMG LLP (United States) ("KPMG") acted together with the 23andMe Defendants as co-principals and/or co-conspirators and/or joint-tortfeasors, and materially contributed to the Data Breach and the violation of customers' privacy. But for the actions, omissions and breaches of duties on the parts of each of the Defendants, the Data Breach would not have occurred. The Data Breach was the product of the Defendants' knowing or, alternatively, reckless, thus willful conduct.

## B. The Plaintiffs

6. The Plaintiff, J. R., is a resident of British Columbia. On or about October 9, 2023, he received a notification email from the Defendants in relation to the Data Breach. J. R. has Eastern European Jewish connections, and was extremely concerned to receive the news that 23andMe's customers' data had been breached and posted on the Dark Web. To date, J. R. has not received meaningful communication from the 23andMe Defendants regarding the impact of the Data Breach on him.
7. The Plaintiff, M. M., is a resident of Ontario. M. M. is an individual with the Ashkenazi Jewish heritage. On or about October 8, 2023, she learned through the media that hackers had curated a list of 1 million Ashkenazi Jewish customers of 23andMe, and were selling that information on the Dark Web. Since then, M. M. has proactively attempted to obtain further information from the 23andMe

Defendants regarding the impact of the Data Breach on her, but those attempts have not been successful. To date, M. M. has not received meaningful communication from the 23andMe Defendants regarding the impact of the Data Breach on her. M. M. has suffered emotional harms as a result of the Data Breach.

### C. The Proposed Class and Sub-Class

8. The Plaintiffs bring this proposed multijurisdictional class proceeding on their own behalf and on behalf of a proposed Class and a proposed Sub-Class, which are defined as follows:

All natural persons residing or domiciled in Canada who provided a bodily substance sample containing their DNA to 23andMe at any time since 23andMe's inception until October 7, 2023;

The Class includes a **Sub-Class** defined as all follows: all such natural persons whose information was subjected to unauthorized access as a result of the Data Breach that affected 23andMe in 2023;

Excluded from the Class are the directors, partners, officers or senior employees of the 23andMe Defendants, KPMG or any of their respective subsidiaries;

(hereinafter, the "**Class**" or "**Class Members**").

### D. The Defendants

#### a) 23andaMe Defendants

9. The 23andMe Defendants provide direct-to-customer genetic testing solutions in Canada.

10. The Defendant 23andMe Holding Co. is an entity continued under the laws of the State of Delaware, and based in South San Francisco, California.
11. 23andMe Holding Co. is a publicly traded company, and its stock is listed for trading on The NASDAQ Global Select Market under the ticker symbol “ME.”
12. The Defendant 23andMe, Inc. is a wholly-owned subsidiary of the Defendant 23andMe Holding Co. It is incorporated under the laws of Delaware, and based in South San Francisco, California.
13. The 23andMe Defendants operate in two reporting business segments: Consumer & Research Services and Therapeutics.
14. In their Consumer and Research Services segment, the 23andMe Defendants offer two types of services:
  - a. first, the Personal Genome Services (“PGS”): The 23andMe Defendants’ PGS services provide customers with a broad suite of genetic reports, including information on customers’ genetic ancestral origins, personal genetic health risks, and chances of passing on certain rare carrier conditions to their children, as well as reports on how genetics can impact responses to medications. These services are offered in various jurisdictions, including in Canada; and
  - b. second, Telehealth services: the 23andMe Defendants provide these services under their Lemonaid subsidiaries division and platform. These services purport to provide patients access to one of the 23andMe Defendants’ affiliated licensed healthcare professionals for medical consultation and treatment for a number of common conditions, and telehealth consultations for certain 23andMe genetic reports.
15. In addition to its customer-facing services and offerings, the 23andMe Defendants engage in research services whereby they use their “vast database of genetic and phenotypic information provided by consenting customers to

discover insights into the genetic origins of disease and to identify targets for drug development.” According to the Defendants, over 80% of their customers elect to participate in the research program.

16. The 23andMe Defendants have monetized customer data for years through licensing them to pharmaceutical development companies. For example, in 2018, the 23andMe Defendants gave license to GlaxoSmithKline (“GSK”), a giant pharmaceuticals company, for US\$300 million. Most recently, on November 3, 2023, days after the reports of the Data Breach, the 23andMe Defendants reported that they had extended a 5-year collaboration with GSK plc licensing 23andMe data for development of pharmaceuticals.
17. The 23andMe Defendants also generate revenue from their customers directly. They provide various tiers of services, and charge customers up to \$398 for their offerings and services, plus additional annual membership fees.
18. The 23andMe Defendants have been providing their offerings and services in Canada since October of 2014.
19. The 23andMe Defendants’ products and offerings are inherently dangerous and potentially harmful, given they deal with extremely sensitive and irreplaceable personal information: genetic and genomic information.
20. Given the inherently dangerous and potentially harmful nature of the 23andMe Defendants’ products and offerings, the Canadian customers of the 23andMe Defendants would not have paid for and used those products and offerings but for the Defendants’ misrepresentations that the 23andMe Defendants used proper data retention and data protection measures and practices.
21. The Data Breach revealed the inherently dangerous and potentially harmful nature of the 23andMe Defendants’ products and offerings and the falsity of the Defendants’ misrepresentations.

22. On March 24, 2025, 23andMe commenced insolvency proceedings under Chapter 11 of the United States Bankruptcy Code, in order to “maximize stakeholder value” and “to facilitate a sale process to maximize the value of its business,” according to 23andMe. These events further revealed the inherently dangerous and potentially harmful nature of 23andMe’s products and offerings, and raised significant concerns regarding the integrity and security of customer data.
23. The 23andMe Defendants have attorned to the jurisdiction of the Courts in British Columbia in relation to these proceedings.

**b) Individual Defendants**

24. **Anne Wojcicki** is a Co-Founder of 23andMe. At the relevant time, she served as the company’s Chief Executive Officer, President, a Director and Chair of the Board of Directors of 23andMe Holding Co. Ms. Wojcicki co-founded 23andMe in 2006 together with two other individuals with the goal of providing common people access to their genetic information.
25. At all material times, Ms. Wojcicki has been aware of the privacy risks and concerns associated with building one of the largest databases of human genome. And she has made representations to the public regarding 23andMe Defendants’ privacy practices. For instance, on or about September 21, 2021, the New York Times published an interview with Ms. Wojcicki, titled “What Is 23andMe Doing With Your DNA?” In this interview, Ms. Wojcicki boasted about 23andMe Defendants’ practices, emphasizing that 23andMe’s structure was built on an “opt-in” basis, and that it “always provide choice and transparency.”
26. At the relevant time, **Roelof Botha** was a director of 23andMe and a member of 23andMe’s Board of Directors’ Audit Committee. According to 23andMe, Mr. Botha focuses on Internet, services and software investments, and he has significant experience being involved with several major tech companies.

27. At the relevant time, **Patrick Chung** was a director of 23andMe and a member of 23andMe's Board of Director's Audit Committee. Mr. Chung is a highly experienced industry professional, having been involved with several major consultancy and tech companies. Mr. Chung hold as joint JD-MBA degree from Harvard Law School and Harvard Business School, and is an attorney admitted to the practice of law in the States of New York and Massachusetts.
28. At the relevant time, **Peter J. Taylor** was a director of 23andMe and a member of 23andMe's Board of Directors' Audit Committee.
29. At the relevant time, **David Baker** was 23andMe's Chief Security Officer. Mr. Baker joined 23andMe in 2020 s Chief Security Officer and Vice President of Engineering, overseeing IT & Security for the company, and purportedly helping it set the industry standard for data privacy and security. Mr. Baker's name has been removed from the Leadership section of 23andMe's website. It is unclear whether or not he continues to hold a senior leadership, or any, position with 23andMe.
30. Mr. Baker has been closely involved with 23andMe's data privacy and cybersecurity efforts, and he has readily acknowledged both: (a) the sensitivity of the information in 23andMe's possession; and (b) the real and significant risk of harm arising from the compromise of that information. In an interview published in June 2021, titled "Data Privacy Is in 23andMe CSO's DNA," Mr. Baker acknowledged the significant value of the information in the possession of the 23andMe Defendants. He furthermore acknowledged the risk of significant harm arising from the compromise of that information, and that it can lead to "a comprehensive identify theft." During this interview, Mr. Baker furthermore made representations to the public regarding 23andMe's purportedly robust data privacy and security measures and practices,
31. The Individual Defendants are highly sophisticated business and industry leaders who have unparalleled experience with the tech industry.

32. As key directors and officers of 23andMe overseeing key and fundamental aspects of 23andMe's business, the Individual Defendants had a duty to affirmatively take steps to ensure 23andMe complied with the applicable standards to safeguard the privacy of its customers' data.
33. Specifically, as part of their duties as officers and directors of 23andMe, the Individual Defendants had the duty to assess the efficacy and propriety of the company's data retention and data protection measures and practices commensurate with the heightened cybersecurity and privacy risks.
34. The Individual Defendants breached their duties, and through action and/or omission, materially contributed to the events leading to the Data Breach and the Data Breach itself.
35. On September 17, 2024, 23andMe's Board of Directors, with the exception of CEO Ms. Wojcicki, resigned *en masse*, citing "a protracted and distracting difference of view with [Ms. Wojcicki] as to the direction of the Company."
36. On March 26, 2025, 23andMe's Co-Founder Linda Avey made a post on X (formerly, Twitter) accusing the Individual Defendants of failing to exercise governance and oversight over 23andMe, which contributed to the downfall of 23andMe and mistreatment of customer data.

**c) KPMG**

**i. KPMG's Engagement with 23andMe**

37. The Defendant KPMG is a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee.
38. At the relevant time, KPMG was the independent auditor of 23andMe from KPMG's offices located in Santa Clara, California.

39. As part of its engagements with 23andMe, KPMG designed, oversaw the design of and/or audited the efficacy and propriety of 23andMe's data retention and data protection practices, whether alone or in conjunction with other persons or entities.
40. At the relevant time, the audit engagement partner of KPMG in relation to 23andMe was Katie Wechsler. Ms. Wechsler has over 20 years of experience working for KPMG in the U.S., the U.K., and Switzerland, serving a wide range of companies, both listed and private. Ms. Wechsler has extensive experience managing the audits of multinational companies within the life sciences, consumer markets, and technology sectors. Her existing client base includes both public and private life sciences companies.

**ii. KPMG Promoted 23andMe and Used Its Relationship with 23andMe to Promote Its Own Business Interests**

41. KPMG has been a promoter of 23andMe Defendants' business, and actively promoted the significant commercial and corporate value in the interconnected genomic and health data they possessed on customers.
42. The KPMG global members' website maintains a dedicated page for life sciences, available at <https://kpmg.com/xx/en/home/industries/life-sciences.html>, which extensively promotes KPMG's services in relation to this sector.
43. Amongst other things, this section of KPMG Global website discusses the "Future of life sciences" and argues: "[t]he future of life sciences will likely be shaped by tech-enabled connectivity, strategic uses of AI, and patient-centric supply chains ... leaders are rethinking their operating models to ensure they can meet stakeholder expectations, anticipate threats, and capitalize on data-driven insights to win in the marketplace."
44. This section of KPMG Global website provides a link to a paper titled "**The future of life sciences; Pressing issues and critical imperatives that will shape the new model for the industry—the connected life sciences company.**" This

paper notes that the development of “precision medicine” with the use of “individuals’ unique genetic profiles and, in some cases, engineers a therapy from a patient’s own cells” as amongst one of the critical signals of the change in the industry, again promoting the commercial capabilities of the exact same kind of data 23andMe Defendants possessed on customers.

45. This paper is co-authored by Larry Raff, a partner with KPMG US, and the KPMG Global Head of Life Sciences and the KPMG US National Market line of business leader. Mr. Raff has over 20 years delivering large scale business, risk and technology transformations to major companies around the world. His focus is on how innovation and changes in market dynamics can help transform outcomes. He has significant depth and expertise in business transformation, process redesign, reactive and predictive risk analysis and innovation-led transformations
46. In a further paper titled “**Driving value from genomics in Life Sciences**,” KPMG International furthermore promotes the significance and usage of the customer data collected and generated by 23andMe Defendants, and argues: “Genomic data [is] the most personal of all human data ... the way such information is gathered, stored, analyzed and used [has] led to a change” in the industry.
47. This paper specifically refers to the licensing arrangements between 23andMe and GSK and promotes the corporate and commercial value in this transaction, noting that the use of the 23andMe Defendants’ data increased the chance of success in the development of pharmaceuticals.
48. This paper is also co-authored by the KPMG Global Head of Life Sciences and the KPMG US National Market line of business leader, Mr. Raff.
49. A further paper published by KPMG member firms titled “**Reshaping the future of pharma: Four critical capabilities for 2030**” further discusses the opportunities and risks in the use of “data-rich” pharmaceutical developments,

and further promotes the significant value of the data collected and generated by 23andMe Defendants.

**iii. KPMG Was Aware of The Data Privacy and Cybersecurity Risks Associated with 23andMe's Business**

50. KPMG member firms have extensively commented on these topics, including without limitation in a paper titled "**Direct-to-consumer genetic testing; Opportunities and risks in a rapidly evolving market,**" which amongst other things acknowledged the privacy risks intertwined with this sector, as follows:

The global direct-to-consumer genetic testing market is growing, fuelled by a rise in awareness, an emerging culture of consumer empowerment, and the demand for increasingly personalized services. However, companies offering these services face increasing concern over data privacy and scientific validity. We advise existing and potential players to focus on building consumer trust, to tailor services to maximize consumer satisfaction, and to work together with regulatory bodies if they hope to thrive in this market.

Direct-to-consumer genetic testing: an exciting market, but not without its challenges.

Once purely the domain of healthcare institutions, rapid technological advancement over the last decade has made it possible for genetic testing to be undertaken cheaply, quickly and directly by consumers.

The global direct-to-consumer genetic testing (DTC-GT) market is forecast to grow steadily to be worth over US\$1bn by 2020<sup>1</sup>, but commercial success for new and more established players is not guaranteed. A set of wide-ranging challenges are likely to become more acute as regulation tightens. For example, growing concerns over data privacy, scientific accuracy, and the psychological impact on consumers demands careful consideration.

Genomic data is special, since it encodes not only our blueprint, but that of our family and children. The continuing privacy and the security of people's genetic data, both immediately, and into the long term, is of paramount importance.

51. The significance of the data privacy and cybersecurity practices was also known to Ms. Wechsler, the KPMG audit partner in charge of the 23andMe engagement. In 2023, at the exact same time that the Data Breach affecting 23andMe was being carried out, Ms. Wechsler made the following post on her public social media:

Fraud, non-compliance and cyber-attacks: These overlapping risks are a triple threat for all organizations. New research from #KPMG suggests that Life Sciences companies may be at greater risk due to overconfidence and underinvestment. Here are five things Life Sciences executives need to know.

#fraud #forensic #lifesciences #investigations #fincrimes  
#financialcrimes

52. Ms. Wechsler's post provided a link to a KPMG paper titled "**Life Sciences: KPMG 2022 Fraud Outlook A triple threat across the Americas**," which found, amongst other things, that "Cyber security is another area for this industry where extensive risk and overconfidence co-exist."

#### **E. The Data Breach**

53. For the purposes of this Consolidated Notice of Civil Claim, the term Data Breach refers to the event, or the sequence of events occurring between April 29, 2023 and September 27, 2023, whereby unauthorized parties exploited the vulnerabilities in the design and structure of the 23andMe Defendants' systems and improperly accessed and obtained highly sensitive and highly valuable personal and health information of the 23andMe Defendants' customers.
54. The Data Breach was first widely reported in the media in early October 2023, following which the 23andMe Defendants commenced an investigation into the Data Breach. On December 5, 2023, the 23andMe Defendants reported that they had completed their investigation into the Data Breach.

#### **F. Customer Data Becomes Available for Sale on Dark Web**

55. The Dark Web is a corner of the internet that is generally not public-facing or available to ordinary audience. The Dark Web participants cannot be readily tracked, and can thus take advantage of anonymity and anonymous activity. Given these features, the Dark Web is actively used by cybercriminals to carry out criminal activities, amongst other purposes.
56. A web posting on the Dark Web, which is attributed to the threat actors, dated October 16, 2023, states and alleges that the threat actor had been able to access and obtain troves of highly sensitive personal and health information of, allegedly, all of the 23andMe Defendants' customers.
57. On or about October 6, 2023, the media reported that customer information of approximately 1 million Ashkenazi Jewish and 100,000 Chinese customers of 23andMe had been made available for sale on the Dark Web. The 23andMe Defendants confirmed those reports.
58. Of note, these reports surfaced at the same time as the conflict in the Middle East was triggered by an attack against Israel, raising significant concerns and distress amongst the Jewish community.
59. According to the alleged hacker, the data stolen and made available for sale on the Ashkenazi Jewish customers of the 23andMe Defendants included such information as profile ID, account ID, first name, last name, sex, birth year, detailed geographic location information as well as genomic data. The hacker further alleged that they possessed information on all of 23andMe Defendants' customers.
60. On or about October 18, 2023, the threat actors made available for sale the highly sensitive personal information of approximately 4.1 million further customers of 23andMe. They, furthermore, claimed that the data set included DNA profiles of the customers, including that of notable public figures and dignitaries.
61. The threat actors claimed the data set included information such as name, date of birth, gender, email and genetic ancestry.

62. It is reported that the threat actor was selling the data for £8 per item, if bought in the blocks of 100,000, or up to \$100 per profile, and that the data included associated email addresses.
63. In the aftermath of these reports, investigative media reported that they had been able to confirm that the 23andMe Defendants' customer data had been made available for sale on the Dark Web as early as on August 11, 2023. According to these reports, a hacker claimed to have 300 terabytes of stolen 23andMe data for sale. The hacker further alleged that they had contacted the 23andMe Defendants, but that the Defendants had not taken the matter seriously. It is reported that the batch of the customer data presented in this incident included genetic data of certain senior Silicon Valley executives.
64. In December 2023, the 23andMe Defendants admitted that the Data Breach had resulted in the compromise of the highly sensitive and valuable personal and health information of at least 6.9 million of their customers.
65. On or about January 25, 2024, the 23andMe Defendants admitted in a regulatory filing with the Attorney General of California that the Data Breach has occurred, and it went unnoticed, from April 29, 2023 through to September 27, 2023.
66. In breach notifications sent to customers in or around January 2024, the 23andMe Defendants also acknowledged that the threat actors were able to access raw genotype or genetics data and health reports.

**G. The Standards Applicable to the 23andMe Defendants in Managing and Safeguarding Customers' Highly Sensitive Personal Information, Which They Violated**

67. The 23andMe Defendants are subject to specific laws, regulations and industry standards and practices to properly manage customer data and to safeguard it against unauthorized access or theft, as detailed below. In broad terms, the applicable standards required the 23andMe Defendants to:

- a. disclose the specific purposes for which they collected customer data and obtain the customer's informed, express consent for such use;
  - b. retain and use the information only for the specified purposes and as long as the information is necessary or required to fulfill such specified purposes;
  - c. dispose of the information once it was no longer required for the specified purposes; and
  - d. while the information remained in the 23andMe Defendants' control, custody or possession, to use appropriate and adequate safeguard measures to protect the information against unauthorized access or theft.
- a) The Standards Applicable to the 23andMe Defendants Under Canadian Law Applicable to Collection and Use of Genetic Information, Which They Violated**
68. On May 4, 2017, Bill S-201, the *Genetic Non-Discrimination Act*, SC 2017, c 3 (“***Genetic Non-Discrimination Act***”) received Royal Assent.
69. The *Genetic Non-Discrimination Act* prohibits any person from requiring an individual to undergo a genetic test or to disclose the existing results of genetic tests. This law empowers customers to retain and exercise control over their personal information, and prohibits all persons from collecting, using or disclosing the genetic test results without the customer's written consent.
70. Furthermore, the *Genetic Non-Discrimination Act* prohibits any person from requiring an individual to undergo a genetic test or disclose the results of a genetic test as a condition of providing goods or services to, entering into or continuing a contract or agreement with, or offering specific conditions in a contract or agreement with, the individual.

**b) The Standards Applicable to the 23andMe Defendants Pursuant to *PIPEDA*, Which They Violated**

71. As entities that are engaged in the collection, use and disclosure of personal information in the course of commercial activities in Canada, the 23andMe Defendants are subject to the *PIPEDA*.
72. The *PIPEDA* applies to entities that are in control of personal information. In this case, the 23andMe Defendants were in control of the Class Members' personal information.
73. Schedule 1 of the *PIPEDA* required that the 23andMe Defendants conduct themselves in accordance with the following statutory duties:
  - a. section 4.1 of Schedule 1 of the *PIPEDA* required that the 23andMe Defendants must be responsible and accountable for personal information, and that they must implement policies and practices to give effect to the principles concerning the protection of personal information;
  - b. section 4.2 of Schedule 1 of the *PIPEDA* required that the 23andMe Defendants must identify the purposes for which personal information was collected at the time or before personal information was collected;
  - c. section 4.3 of Schedule 1 of the *PIPEDA* required that knowledge and consent of the individual Class Members were required for the collection, use or disclosure of personal information, and that the 23andMe Defendants were required to make a reasonable effort to ensure that the individual Class Members were advised of the purposes for which personal information was collected;
  - d. section 4.3.2 of Schedule 1 of the *PIPEDA* required that the individual Class Members' consent be "meaningful," further requiring that "the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed";

- e. sections 4.3.5 and 4.3.8 of Schedule 1 of the *PIPEDA* specified that the Class Members' reasonable expectations were relevant to obtaining consent, and that they ought to have been afforded the opportunity, subject to legal or contractual restrictions and reasonable notice, to withdraw consent;
- f. section 4.5 of Schedule 1 of the *PIPEDA* required that the 23andMe Defendants were not permitted to use or disclose the personal information for any purposes other than those for which it was collected, except with the Class Members' consent;
- g. section 4.5.3 of Schedule 1 of the *PIPEDA* required that the 23andMe Defendants must destroy, erase or anonymize the personal information that was no longer required to fulfill the identified purpose, and that the 23andMe Defendants must develop guidelines and implement procedures to govern the destruction of personal information; and
- h. section 4.7 of Schedule 1 of the *PIPEDA* required that the 23andMe Defendants must protect the personal information by security safeguards appropriate to its sensitivity against loss or theft, as well as unauthorized access, disclosure, use, or modification.

**c) The Standards Applicable to the 23andMe Defendants Pursuant to Their Own Policies, Statements and Representations, Which They Violated**

- 74. The 23andMe Defendants recognize the highly sensitive nature of the information they collect from or on their customers.
- 75. The 23andMe Defendants represent that 23andMe is committed to the robust data privacy and security protections.
- 76. At all material times, the 23andMe Defendants maintained a stated Privacy Statement, which promised and represented that "At 23andMe, Privacy is in our DNA."

77. The 23andMe Defendants' Privacy Statement, furthermore, contained statements and representations substantially as follows:

### **How we use your information**

Now that we've covered the types of information we collect and how we collect it, let's review how we may use it. As a reminder, we will not use your Genetic Information for personalized or targeted marketing and/or advertising without your explicit consent. If you want to dig into the details of how we use your information, check out our [How We Use Your Information page](#).

#### **We use your information to:**

- Provide our Services, including to develop, operate, improve, maintain, and safeguard our Services, including developing new product tools and features
- Analyze and measure trends and usage of the Services
- Communicate with you, including customer support, or to share information about our Services or other offers or information we think may be relevant to you
- Personalize, contextualize and market our Services to you
- Provide cross-context behavioral or targeted advertising (learn more in our [Cookie Policy](#) and [Cookie Choices](#) page)
- Enhance the safety, integrity, and security of our Services, including prevention of fraud and other unauthorized or illegal activities on our Services
- Enforce, investigate, and report conduct violating our Terms of Service or other policies
- Conduct surveys or polls, and obtain testimonials or stories about you
- Comply with our legal, licensing, and regulatory obligations
- Conduct [23andMe Research](#), if you choose to participate

[...]

#### **How does 23andMe protect my information in Research?**

23andMe Research analyses are conducted with information that has been stripped of your identifying Registration Information. You can read more about protections for your data in the [Main Research Consent](#).

[...]

### **Who we *DO NOT* share with:**

You can rest assured, we *will not* voluntarily share your Personal Information with:

- Public databases
- Insurance companies or employers
- Law enforcement, absent a valid court order, subpoena, or search warrant (Check out our track record on this promise in our [Transparency Report](#))

[...]

### **Security Measures**

We implement physical, technical, and administrative measures aimed at preventing unauthorized access to or disclosure of your Personal Information. Our team regularly reviews and improves our security practices to help ensure the integrity of our systems and your Personal Information. To learn more about our practices, please visit our [Customer Care guidance](#).

Please recognize that protecting your Personal Information is also your responsibility. Be mindful of keeping your password and other authentication information safe from third parties, and immediately notify 23andMe of any unauthorized use of your login credentials. Your password is not visible to 23andMe staff, and we encourage you not to share your password with 23andMe or any third parties. 23andMe cannot secure Personal Information that you release on your own or that you request us to release.

[...]

### **Retention of Personal Information**

We retain Personal Information for as long as necessary to provide the Services and fulfill the transactions you have requested, comply with our legal obligations, resolve disputes, enforce our agreements, and other legitimate and lawful business purposes. Because these needs can vary for different data types in the context of different services, actual retention periods can vary significantly based on criteria such as user expectations or consent, the sensitivity of the data, the availability of automated controls that enable users to delete data, and our legal or contractual obligations.

23andMe and/or our contracted genotyping laboratory will retain your Genetic Information, date of birth, and sex as required for compliance with applicable legal obligations, including the federal Clinical Laboratory Improvement Amendments of 1988 (CLIA), California Business and Professions Code Section 1265 and College of American Pathologists (CAP) accreditation requirements, even if you chose to delete your account. 23andMe will also retain limited information related to your account and data deletion request, including but not limited to, your email address, account deletion request identifier, communications related to inquiries or complaints and legal agreements for a limited period of time as required by law, contractual obligations, and/or as necessary for the establishment, exercise or defense of legal claims and for audit and compliance purposes.

**d) The Defendants Violated the Applicable Standards and Their Own Promises and Representations**

78. The 23andMe Defendants violated the standards outlined above and 23andMe's own promises and representations as a result of the following actions and omissions:
  - a. misrepresenting their data retention practices, or otherwise failing to implement proper data retention practices. Specifically, the Defendants retained large troves of highly sensitive and highly valuable customer data that they no longer required to maintain for a valid purpose, and/or otherwise outside of the scope of their authorization; and
  - b. misrepresenting their data protection practices, or otherwise failing to implement proper data protection practices. Specifically, the Defendants failed to introduce, implement and/or maintain appropriate technical, technological and/or procedural measures and controls to safeguard customer data appropriate to the sensitivity of the information and the severity of the risk of cyberattacks.
79. Each of the Individual Defendants and KPMG acted together with the 23andMe Defendants in actions, omissions and breaches of the duties that violated the standards outlined above and 23andMe's own promises and representations.

80. As a result of the Defendants' actions and omissions in breach of their duties, the Defendants enabled, caused or prompted the Data Breach, affirmatively exposing and granting access to the putative Class Members' highly sensitive and highly valuable personal information to unauthorized third parties and cybercriminals.
81. The Defendants' actions and omissions contrary to the standards outlined above and 23andMe's own promises and representations constituted deliberate and purposeful conduct, which was carried out in the context of a for-profit commercial and/or customer relationship with putative Class Members, and in furtherance of or consistent with the Defendants' commercial goals and interests.
  - e) **The Defendants Violated the Applicable Standards Knowingly, Wilfully or Recklessly**
82. The 23andMe Defendants are a publicly traded company involved in the highly sensitive biotechnology sector. The 23andMe Defendants describe themselves as the pioneers in providing in direct-to-consumer genetic testing, and they possess one of the most significant databases of human genome in the world.
83. The Individual Defendants are highly skilled and sophisticated persons with unparalleled experience in the tech and life sciences industry sectors.
84. KPMG is a member of the one of the largest global audit and consultancy firms (one of the "Big 4"), with unparalleled resources and expertise, including in relation to audit, internal controls and governance relevant to computer systems and data management.
85. The Defendants are highly sophisticated corporate and individual actors, who are aware of both the value of the information the 23andMe Defendants collect as well as the value of that information to outside parties, including criminals.
86. The Defendants knew at all times, or they ought to have known, that the trove of highly valuable and sensitive personal information the 23andMe Defendants

collect, generate and store on customers is an extremely attractive target to cybercriminals.

87. The Defendants knew at all times, or they ought to have known, that ~~they~~ the 23andMe Defendants were exposed to a heightened risk of cyberattacks.
88. The Defendants knew at all time, or they ought to have known, that unauthorized access to, or theft of, the highly sensitive customer information in the 23andMe Defendants' possession, power or control would expose the customers to a real and immediate risk of significant privacy harms, damages and losses, including:
  - a. identity theft;
  - b. financial harms, including damages to credit ratings or creditworthiness;
  - c. reputational harms;
  - d. relationship harms; and/or
  - e. physical harms.
89. The data and information security vulnerabilities that enabled the Data Breach were in the design and structure of the 23andMe Defendants' systems. The 23andMe Defendants had made deliberate choices in the design and structure of their systems and website.
90. Furthermore, the 23andMe Defendants were advised of the vulnerabilities in the design and structure of their computer systems, but they chose to disregard those vulnerability reports. The 23andMe Defendants' decision to disregard those reports was deliberate and purposeful.
91. The Data Breach was as such the fruit of the 23andMe Defendants' deliberate and purposeful choices and decisions as to how to design and build their systems, and how to respond (or not to respond) to the reports of vulnerabilities in 23andMe Defendants' computer systems.

92. The Defendants took upon themselves the risk that unauthorized parties or criminals would access or otherwise compromise the highly sensitive and highly valuable customer information in the 23andMe Defendants' power, possession or custody.
93. The Defendants failed to act to protect the putative Class Members' highly sensitive and highly valuable personal information appropriate to the sensitivity of that information and the risks of cyberattacks. The Defendants' actions and omissions were carried out with the knowledge of the real and far-reaching adverse consequences of their breaches of duties.
94. In failing to design and build the systems reasonably free from vulnerabilities, and in failing to reasonably respond to the reports of such vulnerabilities, the Defendants failed to conduct themselves appropriate to the sensitivity of the customer information in their power, possession or custody and the severity of the risk of cyberattacks. The Defendants' conduct was knowing or, alternatively, reckless. The Defendants' conduct was thus willful.

**f) The 23andMe Defendants' Detection and Response to the Data Breach Improper and Inadequate**

95. As part of their overall data accountability, retention and protection practices, the 23andMe Defendants were subject to standards requiring them to detect and respond to any incident of compromise of customer data without delay and in a proper way. The 23andMe Defendants failed to comply with those standards.
96. It is unknown whether the 23andMe Defendants became aware of the Data Breach by themselves or after the media or other third parties reported that their customer data was available for sale on the Dark Web.
97. However, the 23andMe Defendants failed to detect the Data Breach by themselves. There are reports of at least two distinct threat actors who reported that they had identified and exploited the vulnerability in the 23andMe Defendants' systems design and structure between August and October 2023.

Both of them reported that they had reported the vulnerabilities to the 23andMe Defendants, but that the 23andMe Defendants failed to take those issues seriously. The sequence of events suggests that the 23andMe Defendants began investigating the Data Breach later during the first week of October 2023, when the media widely reported that threat actors had accessed and were selling 23andMe customer data on the Dark Web.

98. Given the highly sensitive nature of the customer data, no delay in the detection, response to, or communication regarding the Data Breach would be warranted.
99. Still, it took the 23andMe Defendants several days to acknowledge the Data Breach, and still several more days to communicate regarding the Data Breach with their customers.
100. Yet still, the 23andMe Defendants' communication has been inadequate and inappropriate, as they have failed to provide accurate or complete information to customers regarding what information has been exposed and how customer have been affected.
101. Nor have the 23andMe Defendants provided accurate or complete information regarding the events leading to the Data Breach and the subsequent events.
102. None of that is justified in the circumstances, given the customer data is literally available on the Dark Web.
103. The 23andMe Defendants' improper and inadequate response to the Data Breach indicates that they did not have a proper data security incident response plan.
104. In regulatory filings with the Attorney General of California, filed in January 2024, the 23andMe Defendants acknowledged that the Data Breach had occurred over the span of approximately five months, and that it went undetected, from April through to September 2023.

105. To date, the 23andMe Defendants have not advised customers how and in what ways they have been affected in the Data Breach. Additionally, the 23andMe Defendants have not advised their customers whose information was posted on the Dark Web that they have been affected in such way.

**H. 23andMe Defendants Retained Customer Data Beyond Authorization and In Violation of Their Statutory Obligations**

106. The 23andMe Defendants retained customer data beyond authorization, and without the customers' informed explicit consent in accordance with the standards applicable under the *Genetic Non-Discrimination Act* and the *PIPEDA*.
107. A material purpose and a fundamental value proposition underpinning 23andMe Defendants' business was to monetize on customers' highly valuable genetic and health data. The 23andMe Defendants actively sought to drive commercial value and profit from customer data in their possession.
108. The use of customer data for these purposes was specifically raised with, and commented on by, Ms. Wojcicki in an interview titled "23andMe Admits 'Mining' Your DNA Data Is Its Last Hope," dated February 13, 2024. In this interview, Ms. Wojcicki was quoted as saying "We now have the ability to mine the dataset for ourselves, as well as to partner with other groups. It's a real resource that we could apply to a number of different organizations for their own drug discovery."
109. When asked whether, in her view, "customers are aware that opting in to research also means opting in to giving pharmaceutical partners their data," Ms. Wojcicki refused to provide a direct answer but instead stated as follows: "It's not individual-level data, unless they explicitly consented for individual-level data. I think that most people want to see improvements in their lives," attempting to ascribe an "implied consent" to 23andMe customers.
110. 23andMe Defendants did not, and do not, have the requisite informed, explicit consent of its customers to mine their data for highly profitable pharmaceutical activities. Thus, they accumulated and retained customer data beyond and in

excess of authorization and of purposes other than those contemplated by customers.

### **I. The Defendants' Misrepresentations**

111. The 23andMe Defendants, Individual Defendants and KPMG made both of the misrepresentations alleged herein:

- a. that the 23andMe Defendants employed proper and effective data retention measures and practices; and
- b. that the 23andMe Defendants employed proper and effective data protection measures and practices.

112. 23andMe Defendants and the Individual Defendants made those misrepresentations, whether explicitly or implicitly, and whether by omission or commission, in: (a) 23andMe's Privacy Statement; (b) 23andMe's filings with regulators; and (c) in public statements made by the Individual Defendants, which they made on their own behalf and under the authority and on behalf of 23andMe.

113. KPMG made the foregoing misrepresentations to the public, whether explicitly or implicitly, and whether by omission or commission, in its papers, including those identified herein: (a) "Driving value from genomics in Life Sciences"; and (b) "Reshaping the future of pharma Four critical capabilities for 2030."

114. KPMG furthermore made the foregoing misrepresentations in the presentations, results of factual inquiries and investigations and opinions provided to 23andMe Defendants and their directors and officers, including the Individual Defendants. And those representations were incorporated in 23andMe Defendants and Individual Defendants' statements and regulatory filings.

115. KPMG furthermore made the foregoing misrepresentations to the public, whether explicitly or implicitly, and whether by omission or commission, in KPMG's audit reports, KPMG's audit report on 23andMe dated May 25, 2023 recognized and

represented that 23andMe had proper processes and controls to “provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the company’s assets that could have a material effect on the financial statements.” At all material times, 23andMe’s most significant and valuable asset was the trove of personal and health information, including genetic and genomic information, it possessed on its customers.

116. The Defendants’ misrepresentations were material to the promotion of 23andMe Defendants’ offerings and services. But for the promise of privacy the customers would not provide 23andMe Defendants with their DNA samples and highly sensitive personal and health information.

**J. The Plaintiffs and Putative Class Members Have Suffered Harms, Damages and Losses**

117. The Plaintiffs and putative Class Members have suffered, and will continue to suffer, harms, damages and losses as a result of the Defendants’ misrepresentations and its conduct, as particularized herein.
118. In order to provide their services and offerings, the 23andMe Defendants require and collect highly sensitive personal information on their customers. Additionally, in the course of the customer relationship, and in the normal course of carrying out their business, the 23andMe Defendants generate highly sensitive personal information on their customers.
119. The highly sensitive information the 23andMe Defendants collect from and/or generate on their customers is highly valuable generally and specifically in the context of the within case. Dark Web pricing indices indicate that the personally identifiable information that was affected in the within case can have a Dark Web market price of up to thousands of dollars.
120. The Plaintiffs and putative Class Members entrusted the 23andMe Defendants with their highly sensitive, valuable personal information. But for the Defendants’ promises, representations and statements, the Plaintiffs and putative Class

Members would not have purchased the 23andMe Defendants' offerings or services.

121. The Data Breach was preventable. But for the Defendants' acts, omissions and breaches of the duty in violation of their promises, representations and statements, and but for the Defendants' violation of the standards applicable to them in safeguarding the Class Members' highly sensitive personal information, the Data Breach would not have occurred.
122. The Plaintiffs and the putative Class Members have suffered the following harms, damages and losses:
  - a. economic loss and deprivation equal to the monetary consideration paid for the 23andMe Defendants' offerings and services;
  - b. economic loss and deprivation equal to the "premium" paid for the 23andMe Defendants' offerings and services in order to safeguard customer information;
  - c. loss of valuable, confidential personal and commercial information, all of which is intrinsically valuable;
  - d. damages stemming from, or caused by, identity fraud schemes including, without limitation, damage to credit ratings, damage to perceive credit worthiness, reputation, relationship and other personal and commercial interests;
  - e. non-pecuniary harms, damages and losses as a result of the Data Breach, including emotional distress and anxiety;
  - f. out of pocket expenses required to respond to the consequences of the Data Breach;
  - g. loss of valuable time and resources required to respond to the consequences of the Data Breach; and/or

- h. being exposed to a real risk of significant harm as a result of the exposure of highly sensitive personal and commercial information.

## PART 2: RELIEF SOUGHT

1. On behalf of themselves and the Class, the Plaintiffs seek:
  - a. an order anonymizing the Plaintiffs' identity through initializing their names;
  - b. an order pursuant to all applicable provisions of the *Class Proceedings Act*, RSBC 1996, c. 50, including, but not limited to, sections 2, 4, 4.1, 5, 6, 7, 8, and 10 thereof, certifying this action as a multi-jurisdictional class proceeding and appointing the Plaintiff as the Representative Plaintiff for the Class, as defined here in at page 6, paragraph 13, or such other class definition as may be proposed by the Plaintiff or approved by the Court;
  - c. monetary compensation to the Class for general, compensatory, consequential, symbolic, moral, aggravated, punitive or other forms of damages, whether statutory, at common law and/or equity, on an aggregated basis to the fullest extent possible, for:
    - i. **as against each of the Defendants**, statutory illegality for violations of section 8 of the *Canadian Charter of Rights and Freedoms* and sections 3-5 of the *Genetic Non-Discrimination Act*;
    - ii. **as against each of the Defendants**, breaches of **Provincial Privacy Legislation**:
      1. on behalf of individual Class Members residing in British Columbia, pursuant to section 1 of the *Privacy Act*, RSBC 1996, c. 373, as amended;
      2. on behalf of individual Class Members residing in Manitoba, pursuant to section 2 of *The Privacy Act*, CCSM c P125, as amended;

3. on behalf of individual Class Members residing in Newfoundland and Labrador, pursuant to section 3 of the *Privacy Act*, RSNL 1990, c P-22, as amended;
  4. on behalf of individual Class Members residing in Quebec, pursuant to articles 3 and 35-37 of the *Civil Code of Québec*, CQLR c CCQ-1991, section 5 of the *Charter of Human Rights and Freedoms*, CQLR c C-12, section 10 of the *Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q., c. P-39.1, each as amended; and
  5. on behalf of individual Class Members residing in Saskatchewan, pursuant to section 2 of *The Privacy Act*, RSS 1978, c P-24, as amended;
- iii. **as against each of the Defendants**, the tort of intrusion upon seclusion, on behalf of individual Class Members residing in Canadian Provinces and Territories other than British Columbia, Manitoba, Newfoundland and Labrador, Quebec, and Saskatchewan;
  - iv. **as against each of the Defendants**, negligence, on behalf of all Class Members; and
  - v. **as against each of the Defendants**, pursuant to section 36(1) of the *Competition Act*, RSC 1985, c C-34, breaches of Part VI, section 52, of the *Competition Act*, RSC 1985, c C-34, on behalf of all Class Members;
- d. an order directing a reference or giving such other directions as may be necessary to determine issues not determined at the trial of the common issues;

- e. pre-judgment and post-judgment interest pursuant to the *Court Order Interest Act*, RSBC 1996, c.79;
- f. costs of this action; and
- g. such further and other relief as this Honourable Court may deem just.

### **PART 3: LEGAL BASIS**

#### **A. Statutory Illegality**

- 1. The 23andMe Defendants subjected Canadians to unreasonable search and seizure through unauthorized retention of genetic data as well as unauthorized disclosure of genetic data, without a valid consent, in violation of section 8 of the *Canadian Charter of Rights and Freedoms* and sections 3-5 of the *Genetic Non-Discrimination Act*.
- 2. The Defendants acted as co-principals and/or co-conspirators and/or joint-tortfeasors in the acts and omissions that resulted in the violations of section 8 of the *Canadian Charter of Rights and Freedoms* and sections 3-5 of the *Genetic Non-Discrimination Act*.
- 3. The Defendants made misrepresentations regarding the efficacy and propriety of the 23andMe Defendants' data retention and protection practices, which materially contributed to the violations of section 8 of the *Canadian Charter of Rights and Freedoms* and sections 3-5 of the *Genetic Non-Discrimination Act*.

#### **B. Breaches of Provincial Privacy Legislation**

- 4. On behalf of himself and all other Class Members who are individuals residing in British Columbia, Manitoba, Newfoundland and Labrador, Quebec, and Saskatchewan, the Plaintiff J. R. pleads the statutory rights of action available under the Provincial Privacy Legislation, which are identified in Part 2, para 1(c)(ii) of this Consolidated Notice of Civil Claim.

5. The Defendants violated the Plaintiff J. R.'s and putative Class Members' privacy.
6. The Defendants violated the Plaintiff J. R.'s and putative Class Members' privacy willfully. Specifically, the Defendants' actions and omissions were not appropriate to the sensitivity of the information or the severity of risks of cyberattacks, which were known to the Individual Defendants. As such, the Defendants' conduct was deliberate and purposeful, and it was knowing or, alternatively, reckless.
7. The Defendants violated the Plaintiff J. R.'s and putative Class Members' privacy without a claim of right. Specifically, as the Plaintiff and Class Members had a reasonable expectation—as confirmed in the Defendants' own statements and representations—that the Defendants would properly manage, retain and protect the data. The Defendants had no justification in retaining data beyond the scope of their authorization, and/or in failing to implement proper technical, technological and/or procedural measures and controls to safeguard the putative Class Members' highly sensitive and highly valuable personal information.

#### **C. Tort of intrusion upon seclusion**

8. On behalf of herself and all Class Members who are individuals residing in Canadian jurisdictions that do not have provincial privacy legislation, the Plaintiff M. M. pleads and asserts the tort of intrusion upon seclusion.
9. In support of this claim, the Plaintiff M. M. pleads and asserts that the Defendants intruded upon these Class Members' privacy in a way that was offensive to a reasonable person and caused distress, humiliation, or anguish by:
  - a. misrepresenting 23andMe's data retention measures and practices, or otherwise failing to implement proper data retention practices. Specifically, the 23andMe Defendants retained large troves of highly sensitive and highly valuable customer data that they no longer required to maintain for a valid purpose, and/or otherwise outside of the scope of their authorization; and

- b. misrepresenting 23andMe's data protection measures and practices, or otherwise failing to implement proper data protection practices. Specifically, the 23andMe Defendants failed to introduce, implement and/or maintain appropriate technical, technological and/or procedural measures and controls to safeguard customer data appropriate to the sensitivity of the information and the severity of the risk of cyberattacks.
10. The 23andMe Defendants accumulated, stored, retained, used, and/or disclosed the Plaintiff's and putative Class Members' highly sensitive and highly valuable personal information for reasons other than those reasonably contemplated by putative Class Members.
- D. Negligence**
11. On behalf of themselves and all putative Class Members, the Plaintiffs plead and assert a claim in common law negligence.
12. The Plaintiffs and the putative Class Members were in a special relationship with each of the Defendants as customers of the 23andMe Defendants.
13. The Plaintiffs and the putative Class Members were known or knowable, and identified or identifiable to each of the Defendants.
14. The Defendants owed a duty of care to the Plaintiffs and the putative Class Members to implement proper data retention and data protection measures and practices.
15. The Defendants jointly and materially contributed to the defective state of 23andMe's data privacy and cybersecurity measures and practices either by virtue of designing and/or overseeing the design of, and/or assessing and/or overseeing the assessment or audit of those measures and practices.
16. The Defendants jointly and materially contributed to the misrepresentations made to the wide array of public audience, including the regulators, customers and

23andMe's other stakeholders regarding the propriety and efficacy of 23andMe's data privacy and cybersecurity measures.

17. The Defendants acted as co-principals and/or co-conspirators and/or joint-tortfeasors, in tandem and in an integrated scheme to design, assess, and make material misrepresentations to the public that 23andMe's data privacy and cybersecurity measures were proper and effective, while they were not.
18. Given the risk of data theft, misuse and abuse, the highly sensitive nature of DNA, genetic and genomic data, and the irreplaceable nature of this data, 23andMe's offerings were inherently risky and potentially dangerous and harmful. The Plaintiffs and the Class Members would not have used 23andMe's offerings but for the assurance that 23andMe utilized effective and proper data retention and data protection measures and practices.
19. It was reasonably foreseeable to the Defendants that the Plaintiffs and putative Class Members would suffer harms, damages, and losses if the Defendants breached their promises, statements, representations or otherwise duty of care, which they did.
20. The Defendants were on notice of a heightened risk of cyberattacks against them, and that the Plaintiffs and putative Class Members would suffer severe consequences, harms, losses, and damages if the Defendants breached their duty of care, which they did.
21. The Defendants chose to conduct themselves in a manner that was not appropriate to the sensitivity of customer data and/or the severity of the risk of cyberattacks. The Defendants' conduct was deliberate and purposeful, in furtherance or in the course of conducting their business. It was thus knowing or, alternatively, reckless and, thus, willful.
22. The Plaintiffs and the putative Class Members had no control over the Defendants' decisions and conduct, but trusted that the Defendants would introduce, implement and maintain proper data retention and protection

measures. Indeed, the Defendants promised, stated and represented that they would do so.

23. The Plaintiffs and the putative Class Members suffered harms, damages, and losses as a result of the Defendants' breaches of their duty of care.

**E. Breach of Part VI of the *Competition Act***

24. On behalf of themselves and all other Class Members, the Plaintiffs plead and assert a claim for damages pursuant to section 36 of the *Competition Act* against the Defendants arising out of their violation of Part VI, section 52 of the *Competition Act*.
25. The Defendants made representations to the public that were false or misleading in a material respect regarding the propriety and efficacy of their data retention and data protection measures practices.
26. The Defendants made those false or misleading representations for the purpose of promoting, directly or indirectly, the supply or use of their offerings and services, and/or for the purpose of promoting, directly or indirectly, their business interests, knowingly or recklessly.
27. If and to the extent the Plaintiffs and/or putative Class Members need to prove reliance and/or causation, reliance and causation:
  - a. may be inferred, given the nature and ordinary use of the information with which the Plaintiffs and the putative Class Members entrusted the Defendants;
  - b. may be established directly and by inference based on the Defendants' own statements and representations acknowledging the significance of their privacy and data security obligations commensurate to the putative Class Members' privacy interests, and that they are accordingly subject to rigorous data privacy and data security regulation; and/or

- c. may be established directly by the Plaintiffs and each putative Class Member through individual assessments, which can be done through an efficient and manageable process to be established.

#### **F. The Plaintiffs and Class Members Are Entitled to Compensation**

28. The Plaintiffs and putative Class Members have incurred harms, damages and/or losses as a result of the Defendants' conduct.
29. The Plaintiffs and putative Class Members are entitled to monetary awards or compensation under common law, statutory and/or equitable headings of damages.
30. In the alternative, the Plaintiffs and putative Class Members plead entitlement to compensation under waiver of tort or for disgorgement of profits, and claim an accounting or such other restitutionary relief as may be available for all revenues or profits generated by the Defendants from, as a result of, or reasonably connected with its violations contractually and at law to protect their private information.

Plaintiffs' address for courier service:

**Sage Nematollahi (he/him)**  
**c/o YLAW GROUP**  
410-1122 Mainland Street  
Vancouver, BC V6B 5L1

Place of trial: Vancouver, British Columbia.

The address of the registry is: 800 Smithe Street, Vancouver, BC V6Z 2E1.

Date: October 20, 2023

Amended: \_\_\_\_\_

---

**KND COMPLEX LITIGATION**  
Yonge Eglinton Centre  
Suite 401, 2300 Yonge Street

---

Toronto, Ontario M4P 1E4  
T: (416) 537-3529

**Eli Karp (he/him)**  
[ek@knd.law](mailto:ek@knd.law)

**Sage Nematollahi (he/him)**  
[sn@knd.law](mailto:sn@knd.law)

**YLAW GROUP**  
410-1122 Mainland Street  
Vancouver, BC V6B 5L1  
T: (604) 974-9529

**Leena Yousefi (she/her)**  
[leena@ylaw.ca](mailto:leena@ylaw.ca)

*Counsel to the Plaintiffs*

Rule 7-1(1) of *the Supreme Court Civil Rules* states:

- (1) Unless all parties of record consent or the court otherwise orders, each party of record to an action must, within 35 days after the end of the pleading period,
  - (a) prepare a list of documents in Form 22 that lists
    - (i) all documents that are or have been in the party's possession or control and that could, if available, be used by any party at trial to prove or disprove a material fact, and
    - (ii) all other documents to which the party intends to refer at trial, and
  - (b) serve the list on all parties of record.

**ENDORSEMENT ON ORIGINATING PLEADING OR PETITION  
FOR SERVICE OUTSIDE BRITISH COLUMBIA**

There is a real and substantial connection between British Columbia and the facts alleged in this proceeding. The Plaintiff and the Class Members plead and rely upon the *Court Jurisdiction and Proceedings Transfer Act*, SBC 2003, c 28 (the "CJPTA") in respect of the Defendants. Without limiting the foregoing, a real and substantial connection between British Columbia and the facts alleged in this proceeding exists pursuant to section 10 of the CJPTA because this proceeding:

- (e) concerns contractual obligations, and
  - (i) the contractual obligations, to a substantial extent, were to be performed in British Columbia;
- (f) concerns restitutionary obligations that, to a substantial extent, arose in British Columbia;
- (g) concerns a tort committed in British Columbia; and
- (h) concerns a business carried on in British Columbia.

## APPENDIX

### **Part 1: CONCISE SUMMARY OF NATURE OF CLAIM:**

This is a proposed customer privacy class action arising out of a data breach that affected millions of customers of 23andMe in 2023. As a result of the Data Breach, cybercriminals accessed highly sensitive and highly valuable personal information of 23andMe's customers, including information concerning their ethnicities, religious backgrounds, ancestry roots and connections, and genetics. The Plaintiffs allege that the 23andMe Defendants did not have proper data retention, data protection measures and practices, and that they failed to conduct themselves appropriate to the sensitivity of the customer information in their power, custody or possession, or the severity of the risk of cyberattacks. The Plaintiffs further allege that the Individual Defendants and KPMG acted as co-principals and/or co-conspirators and/or joint-tortfeasors in an integrated scheme, and materially contributed to the design of, and/or assessment and audit of, as well as making representations to the public regarding the propriety and efficacy of, 23andMe's data privacy and cybersecurity measures. The Plaintiffs and the putative Class seek compensation under common law, statutory, and/or equitable headings of damages.

### **Part 2: THIS CLAIM ARISES FROM THE FOLLOWING:**

A personal injury arising out of:

- a motor vehicle accident
- medical malpractice
- another cause

A dispute concerning:

- contaminated sites
- construction defects
- real property (real estate)
- the provision of goods or services or other general commercial matters
- investment losses

- an employment relationship
- a will or other issues concerning the probate of an estate
- a matter not listed here

**Part 3: THIS CLAIM INVOLVES:**

- a class action
- maritime law
- aboriginal law
- constitutional law
- conflict of laws
- none of the above
- do not know

**Part 4: ENACTMENTS RELIED ON:**

1. *Class Proceedings Act*, RSBC 1996, c. 50, as amended
2. *Court Jurisdiction and Proceedings Transfer Act*, RSBC 2003, c.28, as amended
3. *The Canadian Charter of Rights and Freedoms*;
4. *Genetic Non-Discrimination Act*, SC 2017, c 3;
5. *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, as amended
6. *Privacy Act*, RSBC 1996, c. 373, as amended
7. *The Privacy Act*, CCSM c P125, as amended
8. *Privacy Act*, RSNL 1990, c P-22, as amended
9. *Civil Code of Québec*, CQLR c CCQ-1991, as amended
10. *Charter of Human Rights and Freedoms*, CQLR c C-12, as amended
11. *Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q., c. P-39.1, as amended
12. *The Privacy Act*, RSS 1978, c P-24, as amended

13. *Competition Act*, RSC 1985, c C-34, as amended
14. *Court Order Interest Act*, RSBC 1996, c.79, as amended

## Appendix

### THIS APPLICATION INVOLVES THE FOLLOWING:

[Check the box(es) below for the application type(s) included in this application.]

- discovery: comply with demand for documents
- discovery: production of additional documents
- other matters concerning document discovery
- extend oral discovery
- other matter concerning oral discovery
- amend pleadings
- add/change parties
- summary judgment
- summary trial
- service
- mediation
- adjournments
- proceedings at trial
- case plan orders: amend
- case plan orders: other
- experts
- none of the above